Exhibit D: Equipment and Security Requirements:

Fiscal Year – July 1, 2015 to June 30, 2016

Workstation Type	Application	Manufacturer	Specifications

Versadex Desktop	RMS	HP / Dell / IBM or equivalent	Intel or AMD 2 GHz dual core processor
			• Memory
			  ○ 2 GB (minimum)
			  ○ 4 GB (recommended)
			• 20 GB (available) HDD
			• NIC
			  ○ 10 Mbit minimum
			  ○ 100 Mbit recommended
			• 1024x768+ resolution display monitor
			• Microsoft Windows XP, Vista or 7

Versadex Mobile	Field Reporting	Panasonic, Motorola or equivalent	• Intel Centrino dual core processor
			• 2GB RAM
			• Display Resolution
			  ○ 800x600 minimum
			  ○ 1024x768 recommended
			• 13.3” daylight-readable LCD with (preferable) touchscreen
			• 20 GB (available) HDD
			• Microsoft Windows XP, Vista or 7

1. **Access Security** - New, desktop and mobile Equipment with access to the PPDS System must adhere to the following requirements:
   1.1. Both desktop and mobile Equipment shall employ virus protection software
      1.1.1. Use of Anti-Virus and Anti-Spyware software to scan, detect, and eliminate viruses on workstations and laptops
      1.1.2. Anti-Virus and Anti-Spyware software must be kept up to date with current virus definitions, run at start-up, and employ resident scanning
   1.2. Both desktop and mobile Equipment shall apply current operating system service packs and patches; Auto-update is recommended.
   1.3. All desktop and mobile Equipment shall be protected by a current firewall.
   1.4. All mobile Equipment shall employ encryption technology for wireless transmissions from origin to termination. Encryption shall comply with Federal Information Processing Standards (FIPS) publications and guidelines for encryption.

1.5. All mobile Equipment shall employ virtual private network for those transmissions that traverse between wireless local area network and department trusted network segments and shall have a static private IP address.

1.6. All Users shall employ an auto-lock on their workstation or laptop that meets CJIS requirements. RPA is responsible for ensuring that all RPA workstations and MDCs with Access to the System comply with the most current CJIS security policy.

2. **Personnel Security** – Prior to gaining Access to the System's criminal history record information, a person shall:

2.1. Be fingerprinted and a background investigation conducted by the User's RPA.

2.2. That investigation shall include, but not be limited to, verification of information provided by the person and to public record information, including a check of the System's master name file, Oregon LEDS or Washington ACCESS (depending on the state in which the RPA resides) and the National Crime Information Center files, and FBI Criminal Identification files.